



# M&A Due Diligence for a Corporate bolt-on in the Health Industry

ANALYSE



PLAN



DELIVER

OPTIMISE



**Hutton Henry**  
Managing Partner

Working with PE and Portfolio in digital transformation since 2016. Helping tech leaders pre and post deal through coaching and advisory.



**Rod Alderton**  
CIO (Assoc. Partner)

FTSE 250 CIO, Senior IT and digital transformation lead. Helping Investors grow complex technology businesses and identify commercial opportunity.



**Alex Lea**  
CTO/CPO (Assoc. Partner)

High-growth CTO & Digital Product Leader with over 20 years' experience as an advisor & non-exec helping startups and SMEs to avoid common barriers to growth, reach their goals more quickly and at a lower cost.

[www.Beyond-MA.com](http://www.Beyond-MA.com)

## BACKGROUND

Our client, a leading corporation in the Health Industry with operations spread across the globe, primarily in the UK, US, and Australia, was evaluating a bolt-on acquisition in Australia. As a company with significant experience in M&A, they had established integration playbooks and technical architecture blueprints to ensure potential acquisitions would integrate seamlessly into their existing structures. Being in Australia, the potential acquisition demanded an understanding of Australian Privacy Principles and EU GDPR regulations.

## TECHNOLOGY DUE DILIGENCE APPROACH

For this unique case, we deployed our ACT framework but with a few tweaks to suit the unique characteristics of a corporate acquisition. Our focus was not just on technical compatibility but also on the cultural fit between the teams. Moreover, given the potential security risks that could impact the group, data security and management were high on our priority list. We travelled to Australia to meet the management team and understand their business and technical operations.

## ASSISTING PORTFOLIO MANAGEMENT

The technology due diligence uncovered key findings:

1. **Business Systems:** The potential acquisition was utilizing a well-chosen range of known SaaS products supporting their core business. While their existing systems served their candidates well, there was a clear opportunity for system integration and automation to enhance scalability, eliminate errors, and improve data security.
2. **Budget:** The company had a relatively low IT budget, resulting in an insecure tech environment. A temporary CAPEX cost would be associated with moving from MacBooks to corporate Windows machines, and additional spend would be required to improve their cyber security provisions.
3. **Cybersecurity:** A concerning lack of knowledge and investment in cybersecurity led to an insecure environment. Despite implementing two-factor authentication (2FA) on Office 365, the environment was not ready to connect to the group due to the prevalence of unmanaged, unpatched laptops.

## THE CORPORATE M&A DEAL PROCEEDED

Despite the evident cybersecurity gaps, there was an excellent business cultural fit between the two companies. Despite the evident cybersecurity gaps, the two companies had an excellent business-cultural fit. The smaller firm's management was excited about the potential for growth and improved opportunities for staff that would come with being part of a larger entity. They had a hands-on and pragmatic approach to technology and were willing to address the issues identified during the due diligence.

The deal proceeded with a clear understanding from both parties of the technical and cultural implications and requirements for successful integration.